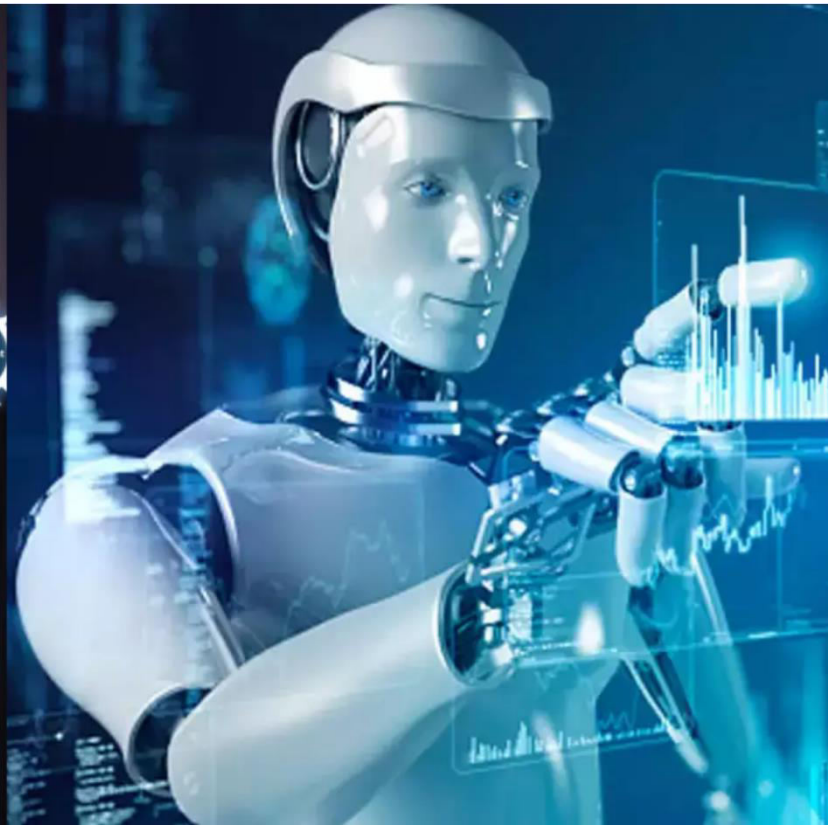
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405279|

Cloud Computing's efficient and Secure Group Sharing and Fine-Grained the Conditional Distribution with Multiple Owners

Navale Nilesh Dagdu

Department of Computer Engineering, Bhabha University, Bhopal, India

ABSTRACT: Cloud computing is becoming a prominent computing paradigm that allows users to store their data into a cloud server to enjoy scalable and on-demand services. Group data sharing in cloud environments has become a hot topic in recent. With the popularity of cloud computing, how to achieve secure and efficient data sharing in cloud environments is an urgent problem to be solved. Although encryption techniques have been used to provide data confidentiality and data security in cloud computing, current technique cannot enforce privacy concerns over encrypted data associated with multiple data owners, which makes co-owners unable to appropriately control whether data distributor can actually distribute their data. In this paper, we propose an Efficient and secure data group sharing and conditional distribution scheme with multi-owner in cloud computing, in which data owner can share private data with a group of users via the cloud in a secure way, and data distributor can distribute the data to a new group of users if the attributes satisfy the access policies in the encrypted data. We further present a multiparty access control mechanism over the distributed encrypted data, in which the data co-owners can append new access policies to the encrypted data due to their privacy preferences.

KEYWORDS: cloud computing, conditional distribution, Data sharing, conditional proxy re-encryption, Encryption, privacy conflict

I. INTRODUCTION

Compared with the traditional information sharing and communication technology, cloud computing has attracted the interest of most researchers because a lot services are provided by the cloud service providers which helps to reduce costs needed for various resources. Cloud storage is one of the most vital service in cloud computing. Scalability is another attracting factor which allows user to scale up and scale down the resources as required. Cloud computing also provides convenient and flexible ways for data sharing. There are two ways to share data in cloud storage. The first case refers to the scenario where one client authorizes access to his/her data for many clients known as one-to-many pattern and the second case refers to a situation in which many clients in the same group authorize access to their data for many clients at the same time known as many-to-many pattern. As the data shared on the cloud is valuable, various security methods are provided by cloud. In current cloud applications various algorithms are used for data encryption and decryption. In encryption is based on ABE [Attribute Based Encryption. Symmetric-key cryptography is used in to enable efficient encryption. Practical group key management algorithm based on a proxy re-encryption technology. In existing system when a user is revoked from a group, he is still able to access files from his previous group which leads to collision attack. Another gap is that a user is not allowed to upload multiple files of same name.

A. Goals/Objectives

1. The main goals of the proposed scheme includes access control, data confidentiality, data security, data sharing and efficiency.
2. To achieve Access Control within the group private keys are generated for every user to provide access to files.
3. To achieve data confidentiality after revocation of any member the private keys of existing members of that group will be updated.
4. To maintain the private keys of every user and provide them access to their resources without any Certificate Authorities.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405279|

B. Problem Statement

In Cloud based group sharing to maintain the data security the private keys of co members of group need to be updated after the revocation of any group member, also to restrict the malicious members from accessing the data in group file upload constraints will be introduced. Data confidentiality will be maintained using double encryption when uploading data on cloud.

II. LITERATURE REVIEW

In this paper [1], we propose a secure exchange of data groups and conditional spreading scheme with multiple owners in cloud computing, where the data owner can share private data with a group of users through the cloud in a secure way and the data communicator can disclose the data to a new group of users if the attributes satisfy the access criteria in the encrypted text. We also present a multipart access control mechanism on the Transmit encrypted text, where data owners can add new policies to access encrypted text due to their privacy preferences In addition, three policy aggregation strategies are provided, including full authorization, owner priority and majority authorization to solve the problem of privacy conflicts caused by different access policies. Safety analysis and experimental results show our scheme is practical and efficient for the secure exchange of data with multiple owners in cloud computing.

In this paper [2], we propose a scheme to check the data access to cloud computing based on data-driven trust owner and reputation generated by a series of reputation it focuses flexibly by applying attributes Encryption and proxy encryption. We integrate the concept of trust assessment and reputation aware of the context in a cryptographic system to support multiple controls scenarios and strategies. The safety and performance of ours the schemes are evaluated and justified by an exhaustive analysis, Safety testing, comparison and implementation. The results shown the efficiency, flexibility and flexibility of our data scheme access control in cloud computing.

In this paper [3], propose a notion called a proxy-assisted encrypted text policy Attribute-based encryption (PA-CPABE), which outsources most decryption calculations to peripheral devices. Respect For the existing ABE with outsourced decryption schemes (ABE-OD), PA-CPABE has the advantage that the distribution of keys It does not require any secure channel. We present a generic construction of PA-CPABE and therefore we demonstrate its security. Moreover, we implement an instance of the proposed PA-CPABE framework to evaluate its performance.

In this paper [4], propose a solution to secure encrypted cloud storages from EDoS attacks and provide resource consumption accountability. It uses CP-ABE schemes in a black-box manner and complies with arbitrary access policy of CP-ABE. We present two protocols for different settings, followed by performance and security analysis.

In this paper [5], describe a framework for data and operation security in IaaS, consisting of protocols for a trusted launch of virtual machines and domain-based storage protection. We continue with an extensive theoretical analysis with proofs about protocol resistance against attacks in the defined threat model. The protocols allow trust to be established by remotely attesting host platform configuration prior to launching guest virtual machines and ensure confidentiality of data in remote storage, with encryption keys maintained outside of the IaaS domain. Presented experimental results demonstrate the validity and efficiency of the proposed protocols. The framework prototype was implemented on a test bed operating a public electronic health record system, showing that the proposed protocols can be integrated into existing cloud environments.

In this paper [6], propose an identity based data group sharing and dissemination scheme in public cloud, in which data owner could broadcast encrypted data to a group of receivers at one time by specifying these receivers' identities in a convenient and secure way. In order to achieve secure and flexible data group dissemination, we adopt attribute-based and timed-release conditional proxy re-encryption to guarantee that only data disseminators whose attributes satisfy the access policy of encrypted data can disseminate it to other groups after the releasing time by delegating a re-encryption key to cloud server. The re-encryption conditions are associated with attributes and releasing time, which allows data owner to enforce fine-grained and timed-release access control over disseminated cipher texts. The theoretical analysis and experimental results show our proposed scheme makes a tradeoff between computational overhead and expressive dissemination conditions.

In this paper [7], based on conditional proxy broadcast re-encryption technology, an encrypted data sharing scheme for secure cloud storage is proposed. The scheme not only achieves broadcast data sharing by taking advantage of

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405279|

broadcast encryption, but also achieves dynamic sharing that enables adding a user to and removing a user from sharing groups dynamically without the need to change encryption public keys. Moreover, by using proxy re-encryption technology, our scheme enables the proxy (cloud server) to directly share encrypted data to the target users without the intervention of data owner while keeping data privacy, so that greatly improves the sharing performance. Meanwhile, the correctness and security is proved, the performance is analyzed and the experimental results are shown to verify the feasibility and efficiency of the proposed scheme.

In this paper [8], they attempt to address this issue and study the scenario when a user shares a photo containing individuals other than himself/herself (termed co-photo for short). To prevent possible privacy leakage of a photo, we design a mechanism to enable each individual in a photo be aware of the posting activity and participate in the decision making on the photo posting. For this purpose, we need an efficient facial recognition (FR) system that can recognize everyone in the photo. However, more demanding privacy setting may limit the number of the photos publicly available to train the FR system. To deal with this dilemma, our mechanism attempts to utilize users' private photos to design a personalized FR system specifically trained to differentiate possible photo co-owners without leaking their privacy. We also develop a distributed consensus based method to reduce the computational complexity and protect the private training set. We show that our system is superior to other possible approaches in terms of recognition ratio and efficiency. Our mechanism is implemented as a proof of concept Android application on Facebook's platform.

This paper [9], propose a bargain based incentive method to resolve the policy conflict problem. We propose a novel pricing system to achieve the balance between privacy loss and sharing benefit. Besides, we introduce a Clark-tax-based punishment mechanism to make sure that no co-owners would act maliciously. Game analysis and user studies are performed to illustrate the effectiveness of our proposed scheme.

Data security [10] issue is one of the main obstacles to the wide application of mobile healthcare social networks (MHSN), since health information is considered to be highly sensitive. In this paper, we introduce a secure data sharing and profile matching scheme for MHSN in cloud computing. The patients can outsource their encrypted health records to cloud storage with identity-based broadcast encryption (IBBE) technique, and share them with a group of doctors in a secure and efficient manner. We then present an attribute-based conditional data re-encryption construction, which permits the doctors who satisfy the pre-defined conditions in the ciphertext to authorize the cloud platform to convert a ciphertext into a new ciphertext of an identity-based encryption scheme for specialist without leaking any sensitive information. Further, we provide a profile matching mechanism in MHSN based on identity-based encryption with equality test, that helps patients to find friends in a privacy-preserving way, and achieve flexible authorization on the encrypted health records with resisting the keywords guessing attack. Moreover, this mechanism reduces the computation cost on patient side. The security analysis and experimental evaluation show that our scheme is practical for protecting the data security and privacy in MHSN.

III. PROPOSED SYSTEM

We achieve fine-grained conditional data distribution over the cipher text in cloud computing with attribute based CPRE. The encrypted data is firstly deployed with an initial access policy customized by data owner. Our proposed multiparty access control mechanism allows the data co-owners to append new access policies to the encrypted data due to their privacy preferences. Hence, the encrypted data can be re-encrypted by the data distributor only if the attributes satisfy enough access policies.

We provide three strategies including full permit, owner priority and majority permit to solve the privacy conflicts problem. Specially, in full permit strategy, data distributor must satisfy all the access policies defined by data owner and co-owners. With the majority permit strategy, data owner can firstly choose a threshold value for data co-owners, and the encrypted data can be disseminated if and only if the sum of the access policies satisfied by data disseminator's attributes is greater than or equal to this fixed threshold.

We prove the correctness of our scheme, and conduct experiments to evaluate the performance at each phase to indicate the effectiveness of our scheme.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405279|

IV. PROJECT MODULES

Group Member: In the proposed scheme, members are people with the same interests (e.g., bidder, doctors, and businessmen) and want to share data in the cloud. The most worrying problem when users store data in the cloud server is the confidentiality of the outsourced data. In this system, users of the same group conduct a key agreement. Subsequently, a common conference key can be used to encrypt the data that will be uploaded to the cloud to ensure the confidentiality of the outsourced data. Attackers or the semi-trusted cloud server cannot learn any content of the outsourced data without the common conference key. In addition, anonymity is also a concern for users. Our scheme uses a technique called group signatures, which allows users in the same group to anonymously share data in the cloud.

Group Manager: is responsible for generating system parameters, managing group members (i.e., uploading member's encrypted data, authorizing group members) and for the fault tolerance detection. The group manager in our scheme is a fully trusted third party to both the cloud and group members. If an external user tries to access files from a different group more than three times then the manager will remove that particular user from the applications.

Cloud: provides users with seemingly unlimited storage services. In addition to providing efficient and convenient storage services for users, the cloud can also provide data sharing services. However, the cloud has the characteristic of honest but curious. In other words, the cloud will not deliberately delete or modify the uploaded data of users, but it will be curious to understand the contents of the stored data and the user's identity.

System Architecture

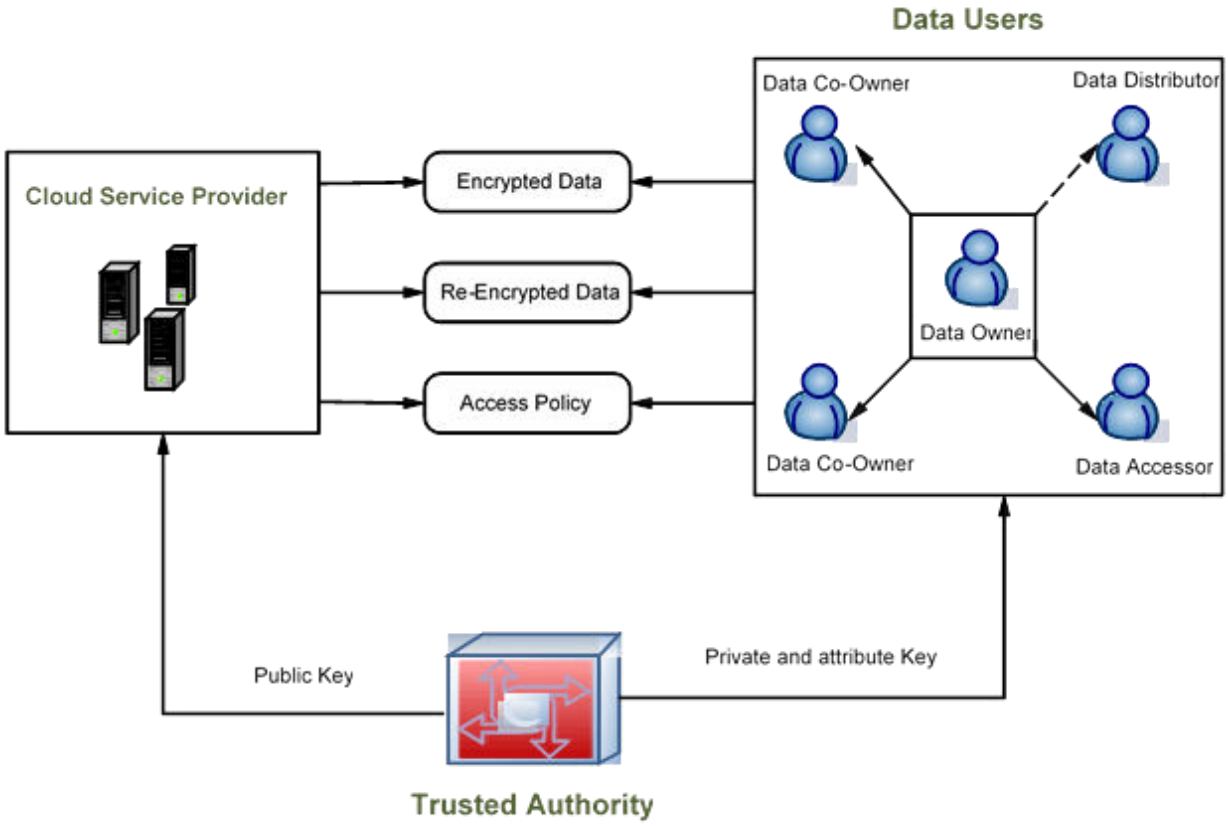


Fig. System Architecture

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405279|

V. CONCLUSION

Data security and privacy is a concern for users in cloud computing In particular, how to apply privacy concerns of multiple owners and protection of data privacy It becomes a challenge. In this paper, present a secure group for data exchange and conditional distribution Multi-owner cloud computing scheme. In our schema, the data owner could encrypt his private data and share them with a group of data access devices simultaneously time conveniently based on the proposed technique. The data owner can specify specific access Attribute-based encrypted text therefore, the encrypted text can be encrypted only by data diffuser whose attributes satisfy the access policy in the encrypted text we also have a multi-part access control mechanism on encrypted text, which allows the co-owners of the data add their access policies to Encrypted text. In addition, provide three aggregation criteria strategies that include full authorization, owner priority and majority help solve the problem of privacy conflicts.

REFERENCES

[1] Qinlong Huang, Member, IEEE, Yixian Yang, Wei Yue and Yue He" Secure Data Group Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing", IEEE TRANSACTIONS ON CLOUD COMPUTING , APRIL 2019

[2] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 485-498, 2017.

[3] H. Cui, X. Yi, and S. Nepal, "Achieving scalable access control over encrypted data for edge computing networks," IEEE Access, vol. 6, pp. 30049–30059, 2018.

[4] K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combining data owner-side and cloud-side access control for encrypted cloud storage," IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 2062–2074, 2018.

[5] N. Paladi, C. Gehrmann, and A. Michalas, "Providing user security guarantees in public infrastructure clouds," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 405-419, 2017.

[6] Q. Huang, Y. Yang, and J. Fu, "Secure data group sharing and dissemination with attribute and time conditions in Public Clouds," IEEE Transactions on Services Computing, 2018.

[7] L. Jiang, and D. Guo "Dynamic encrypted data sharing scheme based on conditional proxy broadcast re-encryption for cloud storage," IEEE Access, vol. 5, pp. 13336 – 13345, 2017.

[8] K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, "My privacy my decision: control of photo sharing on online social networks," IEEE Trans. On Dependable and Secure Computing, vol. 14, no. 2, pp. 199-210, 2017.

[9] L. Fang, L. Yin, Y. Guo, Z. Wang, and Fenzhua Li, "Resolving access conflicts: an auction-based incentive approach," Proc. IEEE Military Communications Conference (MILCOM), pp. 1-6, 2018.

[10] Q. Huang, W. Yue, Y. He, and Y. Yang, "Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing," IEEE Access, vol. 6, pp. 36584–36594, 2018.

[11] S. Wang, K. Liang, J. K. Liu, J. Chen, J. Yu, and W. Xie, "Attribute based data sharing scheme revisited in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 11, no. 8, pp. 1661–1673, 2016.

[12] K. Seol, Y. Kim, E. Lee, Y. Seo, and D. Baik, "Privacy-preserving attribute- based access control model for XML-based electronic health record system," IEEE Access, vol. 6, pp. 9114-9128, 2018.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details